0. Let's see if our ping tool sings—inject some fun and find hidden commands!

Insecure applications can be tricked into running harmful commands, giving attackers control of the system. This happens when user input isn't checked properly. To prevent this, applications need to thoroughly examine all inputs and use secure coding techniques.

Challenge

We're building our Asset Discovery tool and integrating some new features. Before we release it, we need thorough testing. Can you help us ensure it's secure?

This challenge revolves around the Command Injection vulnerability. The `ping` input is vulnerable. Your mission begins with identifying and exploiting the command injection vulnerability in the `ping` functionality.

- Target Application: Asset Discovery tool
- Initial Endpoint: `http://web0x09.hbtn/`

```
Useful instructions:
1. Log into Asset Discovery tool.
2. ping is vulnerable.
3. We can try and give it an input (google.com for example).
4. Flag Location `/0-flag.txt`
```

step one ping google

step two ping google; ls

step three ping google; cat 0-flag.txt